

PATENT ABSTRACTS OF JAPAN

AB

(11)Publication number : 2002-124960

(43)Date of publication of application : 26.04.2002

(51)Int.Cl.

H04L 12/28

H04L 9/08

(21)Application number : 2000-315395

(71)Applicant : LINK EVOLUTION CORP

(22)Date of filing : 16.10.2000

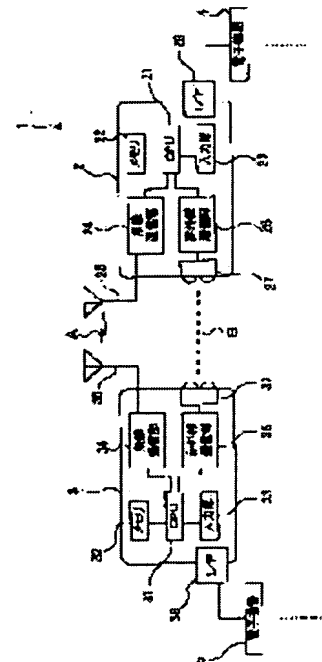
(72)Inventor : KITAKADO KENTARO

(54) COMMUNICATION DEVICE, COMMUNICATION SYSTEM, AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To improve reliability in security without losing the convenience of radio communication when transmitting or receiving data between a plurality of electronic equipment by radio communication.

SOLUTION: In a communication system 1, data are transmitted or received via a radio communication link A conforming to the Bluetooth standard and an infrared communication link B between communication devices 2 and 3. The communication device 2 transmits original encryption information retained in a memory 22 to the communication device 3 via the infrared communication link B, and the communication device 3 retains the transmitted original encryption information in a memory 32. Then, when information is to be transmitted via the radio communication link A from the communication device 2 to the communication device 3, information that is encrypted based on the original encryption information in the memory 22 is transmitted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-124960
(P2002-124960A)

(43) 公開日 平成14年4月26日 (2002. 4. 26)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 B 5 J 1 0 4
9/08		9/00	6 0 1 C 5 K 0 3 3

審査請求 未請求 請求項の数 8 O L (全 14 頁)

(21) 出願番号 特願2000-315395 (P2000-315395)

(22) 出願日 平成12年10月16日 (2000. 10. 16)

(71) 出願人 500225837

リンク・エボリューション株式会社
東京都世田谷区松原3丁目40番7号

(72) 発明者 北角 極太郎

東京都世田谷区松原3丁目40番7号 リン
ク・エボリューション株式会社内

(74) 代理人 100090033

弁理士 荒船 博司 (外1名)

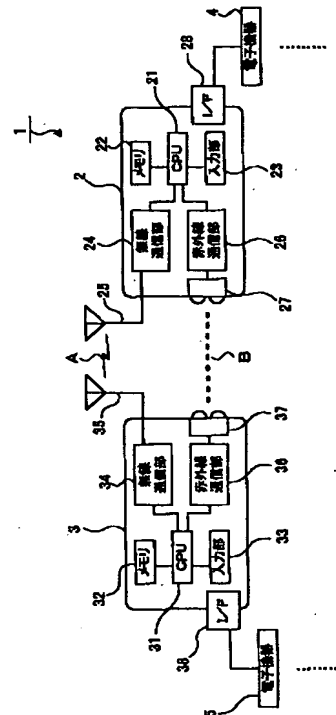
Fターム (参考) 5J104 AA16 EA04 EA21 NA02 NA37
5K033 AA08 CB06 DA17 DA20

(54) 【発明の名称】 通信装置、通信システム、及び、通信方法

(57) 【要約】

【課題】 複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させる。

【解決手段】 通信装置2と通信装置3との間において、Bluetooth規格に準じた無線通信リンクAと、赤外線通信リンクBとを介してデータを送受信する通信システム1であって、通信装置2は、メモリ22内に保持する原始暗号化情報を、赤外線通信リンクBを介して通信装置3へ送信し、通信装置3は、送信された原始暗号化情報を受信してメモリ32内に保持する。そして、通信装置2から通信装置3へ無線通信リンクAを介して情報を送信する場合は、メモリ22内の原始暗号化情報に基づいて暗号化した情報を送信する。



【特許請求の範囲】

【請求項 1】無線信号を送受信する第 1 の通信手段と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段と、暗号化鍵情報を保持する鍵情報保持手段と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第 2 の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって送信させる通信制御手段と、を備えることを特徴とする通信装置。

【請求項 2】前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第 1 の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備えることを特徴とする請求項 1 記載の通信装置。

【請求項 3】前記第 1 の通信手段はブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、前記第 2 の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする請求項 1 または 2 記載の通信装置。

【請求項 4】送信側装置と受信側装置とを備えてなる通信システムであって、前記送信側装置は、無線信号を送受信する第 1 の通信手段と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段と、暗号化鍵情報を保持する鍵情報保持手段と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第 2 の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって前記受信側装置へ送信させる通信制御手段とを備え、前記受信側装置は、前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段と、この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段と、前記送信側装置が有する第 1 の通信手段により送信された情報を受信する暗号化情報受信手段とを備えること、を特徴とする通信システム。

【請求項 5】前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第 1 の通信手段による無線信号の送受信を拒否する通信拒否手段をさらに備えることを特徴とする請求項 4 記載の通信システム。

【請求項 6】前記送信側装置が有する第 1 の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース規格に準じた通信方式により無線信号を送受信するものであって、前記送信側装置が有する前記第 2 の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする請求項 4 または 5 記載の通信システム。

【請求項 7】前記送信側装置が有する鍵情報送信制御手段は、前記暗号化鍵情報を暗号化して前記第 2 の通信手段によって送信させることを特徴とする請求項 4 から 6 のいずれかに記載の通信システム。

【請求項 8】無線信号を送受信する第 1 の通信手段と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段とを有する送信側装置と、受信側装置とを備えてなる通信システムにおける通信方法であって、前記送信側装置により、暗号化鍵情報を前記第 2 の通信手段によって前記受信側装置へ送信する工程と、前記受信側装置により、前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって前記受信側装置へ送信する工程と、を含むことを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、異なる複数の通信方式に対応する通信装置、この通信装置を備える通信システム、及び、この通信システムにおける通信方法に関する。

【0002】

【従来の技術】従来、パーソナルコンピュータ、PDA (Personal Digital Assistant)、携帯電話機等の電子機器間でデータ通信を行う場合には、互いの電子機器をケーブルで接続する手法が用いられていた。しかし、ケーブルを用いた手法は、電子機器にケーブルを接続する手間がかかり、ケーブルを携帯しなければならないため、不便であった。そこで、最近では、複数の電子機器間におけるデータ通信に無線通信技術が用いられるようになった。

【0003】特に、近年では、電子機器の利便性を向上させるため、互換性に富む複数の無線通信規格が策定されている。これらの通信規格に準じた通信装置を用いれば、様々な電子機器との間でデータ通信を容易に行うことができる。

【0004】

【発明が解決しようとする課題】しかしながら、無線通信技術を利用してデータ通信を行う場合は、データの漏

10

20

30

40

50

洩に注意する必要があった。特に、様々な機器との間で通信可能な通信規格に準じている場合は、誤って無関係な他の機器によってデータが受信されないように注意する必要があった。このように、無線通信技術を用いたデータ通信では、セキュリティ上の信頼性を向上することが課題となっていた。

【0005】本発明の課題は、複数の電子機器間で無線通信によってデータを送受信する場合に、無線通信の利便性を損なうことなくセキュリティ上の信頼性を向上させることである。

【0006】

【課題を解決するための手段】本発明は、このような課題を解決するために、次のような特徴を備えている。なお、次に示す手段の説明中、括弧書きにより実施の形態に対応する構成を一例として示す。符号等は、後述する図面参照符号等である。

【0007】請求項1記載の発明の通信装置(2)は、無線信号を送受信する第1の通信手段(例えば、図1に示す無線通信部24)と、この第1の通信手段とは異なる通信方式により信号を送受信する第2の通信手段(例えば、図1に示す赤外線通信部26)と、暗号化鍵情報を保持する鍵情報保持手段(例えば、図2に示す原始暗号化情報格納領域101を有するメモリ22)と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第2の通信手段によって他の通信装置へ送信させる鍵情報送信制御手段(例えば、図3(a)に示す処理を行うCPU21)と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第1の通信手段によって送信させる通信制御手段(例えば、図5に示す処理を行うCPU21)とを備えることを特徴とする。

【0008】この請求項1記載の発明によれば、無線信号を送受信する第1の通信手段と、この第1の通信手段とは異なる通信方式により信号を送受信する第2の通信手段とを備え、鍵情報保持手段により、暗号化鍵情報を保持し、この鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段の制御により、第2の通信手段によって他の通信装置へ送信するとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第1の通信手段によって送信するので、この通信装置により送信される情報は、第2の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信することができる。これにより、第1の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第1の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により情報が受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第2の通信手段によって送信

される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【0009】請求項2記載の発明は、請求項1記載の通信装置において、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、前記第1の通信手段による無線信号の送受信を拒否する通信拒否手段(例えば、図5のステップS45に示す処理を行うCPU21)をさらに備えることを特徴とする。

【0010】請求項2記載の発明によれば、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第1の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿性をより確実に保持することができる。

【0011】請求項3記載の発明は、請求項1または2記載の通信装置において、前記第1の通信手段はブルートゥース(Bluetooth)規格に準じた通信方式により無線信号を送受信するものであって、前記第2の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする。

【0012】請求項3記載の発明によれば、第1の通信手段はブルートゥース(Bluetooth)規格に準じた通信方式により無線信号を送受信するものであり、第2の通信手段は、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース(Bluetooth)規格の無線通信において、情報の秘匿性を確保することができる。特に、第2の通信手段に赤外線信号を用いた通信方式を利用するので、第2の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるので、情報の秘匿性をより一層高めることができる。

【0013】請求項4記載の発明は、送信側装置(例えば、図1に示す通信装置2)と受信側装置(例えば、図1に示す通信装置3)とを備えてなる通信システム

(1)であって、前記送信側装置は、無線信号を送受信する第1の通信手段(例えば、図1に示す無線通信部24)と、この第1の通信手段とは異なる通信方式により信号を送受信する第2の通信手段(例えば、図1に示す赤外線通信部26)と、暗号化鍵情報を保持する鍵情報保持手段(例えば、図2に示す原始暗号化情報格納領域101を有するメモリ22)と、この鍵情報保持手段に保持された暗号化鍵情報を、前記第2の通信手段によって前記受信側装置へ送信させる鍵情報送信制御手段(例

えば、図 3 (a) に示す処理を行う CPU 2 1) と、前記鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって前記受信側装置へ送信させる通信制御手段 (例えば、図 5 に示す処理を行う CPU 2 1) とを備え、前記受信側装置は、前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信する鍵情報受信手段 (例えば、図 1 に示す赤外線通信部 3 6、及び図 3 (b) に示す処理を行う CPU 3 1) と、この鍵情報受信手段により受信された暗号化鍵情報を保持する受信鍵情報保持手段 (例えば、図 1 に示すメモリ 3 2) と、前記送信側装置が有する第 1 の通信手段により送信された情報を受信する暗号化情報受信手段 (例えば、図 1 に示す無線通信部 3 4) とを備えることを特徴とする。

【 0 0 1 4 】請求項 4 記載の発明によれば、送信側装置と受信側装置とを備えてなる通信システムであって、送信側装置は、無線信号を送受信する第 1 の通信手段と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段とを備え、鍵情報保持手段により暗号化鍵情報を保持し、鍵情報保持手段に保持された暗号化鍵情報を、鍵情報送信制御手段によって、第 2 の通信手段によって受信側装置へ送信させるとともに、通信制御手段の制御によって、鍵情報保持手段に保持された暗号化鍵情報をもとに情報を暗号化して、第 1 の通信手段によって受信側装置へ送信し、受信側装置は、送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を鍵情報受信手段によって受信し、鍵情報受信手段により受信された暗号化鍵情報を受信鍵情報保持手段によって保持し、送信側装置が有する第 1 の通信手段により送信された情報を暗号化情報受信手段によって受信する。

【 0 0 1 5 】また、請求項 8 記載の発明は、無線信号を送受信する第 1 の通信手段 (例えば、図 1 に示す無線通信部 2 4) と、この第 1 の通信手段とは異なる通信方式により信号を送受信する第 2 の通信手段 (例えば、図 1 に示す赤外線通信部 2 6) とを有する送信側装置 (例えば、図 1 に示す通信装置 2) と、受信側装置 (例えば、図 1 に示す通信装置 3) とを備えてなる通信システム

(1) における通信方法であって、前記送信側装置により、暗号化鍵情報を前記第 2 の通信手段によって前記受信側装置へ送信する工程と、前記受信側装置により、前記送信側装置が有する第 2 の通信手段により送信された暗号化鍵情報を受信して記憶する工程と、前記送信側装置により、前記暗号化鍵情報をもとに情報を暗号化して、前記第 1 の通信手段によって前記受信側装置へ送信する工程とを含むことを特徴とする。

【 0 0 1 6 】従って、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第 1 の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性

を確保することができる。特に、第 1 の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第 2 の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【 0 0 1 7 】請求項 5 記載の発明は、請求項 4 記載の通信システムにおいて、前記送信側装置は、前記鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、前記受信側装置が有する受信鍵情報保持手段に保持されていない場合に、前記第 1 の通信手段による無線信号の送受信を拒否する通信拒否手段 (例えば、図 5 のステップ S 4 5 に示す処理を行う CPU 2 1) をさらに備えることを特徴とする。

【 0 0 1 8 】請求項 5 記載の発明によれば、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第 1 の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、情報の秘匿をより確実に保持することができる。

【 0 0 1 9 】請求項 6 記載の発明は、請求項 4 または 5 記載の通信システムにおいて、前記送信側装置が有する第 1 の通信手段と、前記受信側装置が有する暗号化情報受信手段とは、ブルートゥース (Bluetooth) 規格に準じた通信方式により無線信号を送受信するものであって、前記送信側装置が有する前記第 2 の通信手段と、前記受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信することを特徴とする。

【 0 0 2 0 】請求項 6 記載の発明によれば、送信側装置が有する第 1 の通信手段と、受信側装置が有する暗号化情報受信手段とは、ブルートゥース (Bluetooth) 規格に準じた通信方式により無線信号を送受信するものであって、送信側装置が有する第 2 の通信手段と、受信側装置が有する鍵情報受信手段とは、赤外線信号を用いた通信方式により無線信号を送受信するので、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース (Bluetooth) 規格の無線通信において、情報の秘匿性を確保することができる。特に、第 2 の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第 2 の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに

近接し、かつ所定の立体角以内で対向する必要があるの
で、情報の秘匿性をより一層高めることができる。

【0021】請求項7記載の発明は、請求項4から6の
いずれかに記載の通信システムにおいて、前記送信側装
置が有する鍵情報送信制御手段は、前記暗号化鍵情報を
暗号化して前記第2の通信手段によって送信させること
を特徴とする。

【0022】請求項7記載の発明によれば、送信側装置
が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化
して第2の通信手段によって送信させるので、暗号化鍵
情報を送信する際の情報の漏洩をより確実に防止でき
る。これにより、セキュリティ上の信頼性をより一層高
めることができる。

【0023】

【発明の実施の形態】以下、図を参照して本発明の実施
の形態を詳細に説明する。

【0024】〔第1の実施の形態〕図1は、本発明を適
用した第1の実施の形態としての通信システム1の構成
を示すブロック図である。同図に示すように、通信シス
テム1は、互いに通信可能な通信装置2及び通信装置3
により構成される。通信装置2と通信装置3との間に
は、無線電波を媒体とする無線通信リンクAと、赤外線
を利用した赤外線通信リンクBとが形成される。

【0025】なお、図1に示す通信装置2及び通信装置
3は、いずれも同一構成によってなる通信装置である
が、本第1の実施の形態においては、通信装置2をアク
セス要求側の装置、通信装置3をアクセス受信側の装置
として説明する。

【0026】通信装置2は、CPU (Central Processi
ng Unit) 21、メモリ22、入力部23、無線通信部
24、アンテナ25、赤外線通信部26、赤外線受発光
ユニット27、及びインターフェース部28の各部を備
えて構成される。

【0027】CPU21は、入力部23における指示操
作に従って、メモリ22に格納されたシステムプログラ
ムを読み出して実行し、通信装置2の各部を駆動制御す
る。具体的には、CPU21は、メモリ22内のプログ
ラムに従って、無線通信部24を制御し、通信装置3と
の間に無線通信リンクAを確立する。続いてCPU21
は、赤外線通信部26及び赤外線受発光ユニット27に
よって赤外線通信リンクBを確立する。そして、CPU
21は、赤外線通信リンクBを介して、メモリ22内に
格納された暗号化に関する各種情報を通信装置3へ送信
する。

【0028】その後、CPU21は、通信装置3から赤
外線通信リンクBを介して送信された情報を受信し、情
報の内容を確認して、通信装置3との間の無線通信リン
クA及び赤外線通信リンクBを切断する。

【0029】また、CPU21は、入力部23から入力
される指示に従って、無線通信部24を制御し、通信装

置2の近辺に存在する通信装置をスキャンするための無
線信号をアンテナ25から出力させる。このスキャン動
作により、無線通信回線を介して接続可能な通信装置が
検出された場合には、検出された通信装置から送信され
た情報を無線通信部24によって受信して解析する。

【0030】そして、受信した情報をメモリ22内に格
納された原始暗号化情報と照合し、一致した場合には接
続を許可して、該検出された通信装置との間で無線通信
を開始する。また、受信した情報が原始暗号化情報と一
致しない場合には、該通信装置との間の通信を拒否す
る。

【0031】メモリ22は、EEPROM、フラッシュ
メモリ等の不揮発性記憶素子を備えて構成される。メモ
リ22は、CPU21により実行されるシステムプログ
ラム等のプログラム、及び、これらプログラムに係るデ
ータ等を格納する。また、メモリ22は、CPU21に
より処理されるデータや、入力部23から入力されたデ
ータ等を一時的に保持する。

【0032】ここで、メモリ22に格納されるデータに
ついて説明する。図2は、メモリ22内部の構成を模式
的に示す図である。メモリ22内には、上記各種プログ
ラムを格納した格納領域(図示略)の他、図2に示すよ
うに原始暗号化情報格納領域101及び転送諸元情報格
納領域102が設けられる。

【0033】原始暗号化情報格納領域101には、暗号
化の際の「鍵」として使用される暗号化鍵情報、及び、
暗号化鍵情報を他の電子機器に対して送信した履歴等
を含む暗号化鍵管理情報が格納される。原始暗号化情報
格納領域101に格納される各種情報を、原始暗号化情報
と総称する。

【0034】この原始暗号化情報格納領域101に格納
される原始暗号化情報は、予め原始暗号化情報格納領域
101に格納されているものとしても良いし、入力部2
3の操作によって、随時入力されるようにしても良い。

【0035】また、転送諸元情報格納領域102には、
通信装置2の製品情報、固有機能情報、使用者情報、シ
リアルNo.等の各種情報が格納される。これらの転送諸
元情報格納領域102に格納される各種情報を、転送諸
元情報と総称する。なお、転送諸元情報格納領域102
に格納される情報は、予めメモリ22に格納されている
ものとしても良いし、入力部23の操作によって入力さ
れるものとしても良く、或いは、インターフェース部2
8に接続された電子機器4から入力されるものとしても
良い。

【0036】入力部23は、それぞれ入力可能な情報が
割り当てられた複数のキー等の入力デバイスを備えてお
り、操作内容に対応する操作信号を生成してCPU21
へ出力する。

【0037】無線通信部24は、エンコーダ、デコー
ダ、RF、アンプ等を内蔵しており、CPU21から入

10

20

30

40

50

力される信号を変換して無線信号を生成し、アンテナ25を介して通信装置3へ送信する。また、無線通信部24は、通信装置3から送信された無線信号をアンテナ25によって受信し、受信した無線信号を変換して得られる信号をCPU21へ出力する。

【0038】ここで、無線通信部24としては、例えば、ブルートゥース (Bluetooth) 規格に準じた無線通信ユニットが挙げられる。Bluetooth規格とは、通信機器、電子機器、ソフトウェア等を製造する事業者が複数集まって構成されるプロモーターと、Bluetooth SIG (Special Interest Group) により策定された無線通信規格である。Bluetooth規格では、2.4GHz (ギガヘルツ) 帯の周波数の無線信号を利用して、およそ数メートル以内の複数の電子機器間で無線通信を行う。

【0039】Bluetooth規格に準じた無線通信ユニットを搭載した電子機器は、互いにピコネットと呼ばれるグループを形成する。そして、同一のピコネットに属する電子機器間で相互に通信することが可能である。同一のピコネットには多くの電子機器が同時に属することができる。また、1台の通信装置が同時に複数のピコネットに属することも可能である。このため、携帯型電話機を始め、パーソナルコンピュータ、PDA (Personal Digital Assistant) と呼ばれるハンドヘルドコンピュータ、プリンタ、音楽プレーヤ等の様々な機器を互いに接続する通信方式として注目されている。以下、無線通信部24は上記Bluetooth規格に準じた通信ユニットであり、無線通信部24及びアンテナ25を利用して実行される無線通信 (無線通信リンクAを介した無線通信) は、Bluetooth規格に準じた2.4GHz帯の電波により行われるものとして説明する。

【0040】赤外線通信部26は、エンコーダ、デコーダ等を内蔵しており、赤外線受発光ユニット27に接続されている。赤外線通信部26は、CPU21から入力された信号を変換して赤外線受発光ユニット27へ出力する。赤外線受発光ユニット27は、LED (Light Emitting Diode) やフォトセンサ等を内蔵し、赤外線通信部26から入力された信号をもとに内蔵するLEDを発光させ、赤外線信号として通信装置3へ向けて出力する。

【0041】また、赤外線受発光ユニット27は、内蔵するフォトセンサによって通信装置3からの赤外光を受光すると、受光パターンを所定の信号に変換して赤外線通信部26へ出力する。さらに、赤外線通信部26は、赤外線受発光ユニット27から入力される信号を変換して、CPU21へ出力する。

【0042】インターフェース部28は、通信装置2と、通信装置2の外部の電子機器とを接続するためのインターフェースであって、コネクタ等を備えている。ここで、インターフェース部28に接続される電子機器5としては、例えば、携帯型電話機やパーソナルコンピュ

ータ、PDA等が挙げられるが、特に限定されるものではない。また、通信装置2は、図示しないリチウムイオン電池やニッケル-カドミウム電池等の二次電池、もしくは乾電池等を内蔵し、これらの電池を電源として動作するが、通信装置2に電池を内蔵せずに、インターフェース部28を介して通信装置2へ電源が供給される構成としても良い。

【0043】さらに、通信装置2が有する入力部23に代えて、インターフェース部28に接続された機器が具備する入力装置を用いる構成としても良い。この場合、CPU21は、インターフェース部28に接続された機器から入力される信号に従って動作すれば良く、入力部23を備えていなくても良い。

【0044】次いで、通信装置3の構成について説明する。通信装置3は、CPU31、メモリ32、入力部33、無線通信部34、アンテナ35、赤外線通信部36、赤外線受発光ユニット37、及びインターフェース部38の各部を備えて構成される。ここで、上記メモリ32、入力部33、無線通信部34、アンテナ35、赤外線通信部36、赤外線受発光ユニット37、及びインターフェース部38の各部は、通信装置2が有するメモリ22、入力部23、無線通信部24、アンテナ25、赤外線通信部26、赤外線受発光ユニット27、及びインターフェース部28の各部と同一の構成によってなるものであり、説明を省略する。

【0045】CPU31は、入力部33における指示操作に従って、メモリ32に格納されたシステムプログラムを読み出して実行し、通信装置3の各部を駆動制御する。具体的には、CPU31は、メモリ32内のプログラムに従って、無線通信部34を制御し、通信装置2との間に無線通信リンクAを確立する。

【0046】続いてCPU31は、赤外線通信部36及び赤外線受発光ユニット37によって赤外線通信リンクBを確立する。そして、CPU31は、通信装置2が有する赤外線受発光ユニット27から発せられた赤外線信号を赤外線受発光ユニット37によって受光し、通信装置2から送信された暗号化に関する各種情報を受信する。

【0047】ここで、CPU31は、通信装置2から送信された各種情報をメモリ32内に格納するとともに、該情報を、赤外線通信部36及び赤外線受発光ユニット37を介して通信装置2へ送信する。そして、通信装置2が有するアンテナ25から出力された無線信号を受信し、受信した信号が無線通信リンクA及び赤外線通信リンクBの切断を要求している場合は、通信装置2との間の無線通信リンクA及び赤外線通信リンクBを切断する。

【0048】次に、本実施の形態の動作を説明する。図3は、本第1の実施の形態における通信システム1の動作を示すフローチャートである。図3(a)は、アクセ

ス要求側の装置、すなわち通信装置 2 の動作を示し、図 3 (b) はアクセス受信側の装置、すなわち通信装置 3 の動作を示す。なお、図中、実線矢印で示す信号は、無線通信リンク A (図 1) を介して送受信される上記 Bluetooth 規格に準じた無線信号であり、破線矢印で示す信号は、赤外線通信リンク B (図 1) を介して送受信される赤外線信号である。

【0049】まず、図 3 (a) に示すように、CPU 21 は、入力部 23 からの指示入力に従って動作を開始し、通信装置 3 に対して接続を求める接続要求信号を生成して、無線通信部 24 によって通信装置 3 へ送信させる (ステップ S11)。

【0050】CPU 31 は、入力部 33 からの指示入力によって動作を開始し、無線通信部 34 によって通信装置 2 から送信される無線信号を受信可能な状態に移行する。そして、無線通信部 24 から送信された接続要求を無線通信部 34 によって受信すると (ステップ S21)、接続の確認となる接続確認信号を生成し、無線通信部 34 によって送信させる (ステップ S22)。

【0051】CPU 21 は、CPU 31 の制御により無線通信部 34 から送信された接続確認信号を無線通信部 24 によって受信すると (ステップ S12)、メモリ 22 の転送諸元情報格納領域 102 に格納された転送諸元情報を読み出して、赤外線通信部 26 及び赤外線受発光ユニット 27 によって、赤外線信号として通信装置 3 へ送信させる (ステップ S13)。

【0052】CPU 31 は、通信装置 2 の赤外線通信部 26 により赤外線信号として送信された転送諸元情報を、赤外線通信部 36 によって受信すると (ステップ S23)、メモリ 32 の転送諸元情報格納領域 102 に格納された転送諸元情報を読み出して、赤外線通信部 36 によって送信させる (ステップ S24)。

【0053】CPU 21 は、通信装置 3 から送信された転送諸元情報を赤外線通信部 26 によって受信すると (ステップ S14)、メモリ 22 内の原始暗号化情報格納領域 101 に格納されている原始暗号化情報を読み出して、赤外線通信部 26 によって通信装置 3 へ送信させる (ステップ S15)。

【0054】CPU 31 は、通信装置 2 から送信された原始暗号化情報を受信すると (ステップ S25)、受信した原始暗号化情報をメモリ 32 内の原始暗号化情報格納領域 101 に記憶させる (ステップ S26)。なお、ここで、予めメモリ 32 の原始暗号化情報格納領域 101 に格納されていた原始暗号化情報については、新たに受信した原始暗号化情報により上書きされるものとしても良いし、或いは、新たに受信した原始暗号化情報とは異なる領域に保存されるものとしても良い。

【0055】続いて、CPU 31 は、ステップ S25 で受信し、メモリ 32 内の原始暗号化情報格納領域 101 に記憶した原始暗号化情報を、赤外線通信部 36 によ

て通信装置 2 へ送信する (ステップ S27)。

【0056】CPU 21 は、通信装置 3 から送信された原始暗号化情報を受信すると (ステップ S16)、受信した原始暗号化情報と、メモリ 22 の原始暗号化情報格納領域 101 に格納されている原始暗号化情報とを照合し、一致することを確認する (ステップ S17)。すなわち、ステップ S15 で通信装置 3 へ送信した原始暗号化情報と、通信装置 3 から送信された原始暗号化情報とが一致することを確認することにより、ステップ S15, S16, S25, S26 における原始暗号化情報の送受信が問題なく実行されたことを確認する。

【0057】そして、CPU 21 は、通信の切断を要求する切断要求信号を生成して、無線通信部 24 によって通信装置 3 へ送信させる (ステップ S18)。CPU 31 は、通信装置 2 から送信された切断要求信号を無線通信部 34 によって受信すると (ステップ S28)、切断要求の受信を確認する切断確認信号を生成して、無線通信部 34 によって通信装置 2 へ送信させ (ステップ S29)、本処理を終了する。

【0058】また、CPU 21 は、通信装置 3 から送信された切断確認信号を無線通信部 24 によって受信すると (ステップ S19)、本処理を終了する。

【0059】以上の図 3 に示す処理によって、通信装置 2 が有するメモリ 22 と、通信装置 3 が有するメモリ 32 とは、予めメモリ 22 内の原始暗号化情報格納領域 101 に格納されていた原始暗号化情報を格納した状態になる。

【0060】図 3 に示す処理においては、転送諸元情報および原始暗号化情報が、赤外線通信リンク B (図 1) を介して送受信される。一般に、赤外線信号による無線通信を行う場合、通信を行う電子機器が互いに近接しており、かつ、互いの電子機器が有する赤外線受発光部が対向していることが必要である。特に、互いの電子機器が有する赤外線受発光部は、比較的狭い立体角に収まるように対向していなければならず、無関係な電子機器により傍受される可能性は低く、セキュリティ上の懸念は小さいものである。しかしながら、以下に述べる暗号化を施すことにより、赤外線通信リンク B を介した通信におけるセキュリティ上の信頼性をより確実なものとすることができる。

【0061】図 4 (a) には、暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを図示する。また、図 4 (b) には、赤外線通信におけるデータユニットの構成を模式的に示す。

【0062】一般に、赤外線通信においては、データリンク層、リンクマネージメント層、トランスポート層における互換性を保持していれば、それより上位の階層におけるサービス・データ・ユニットを暗号化しても、プロトコル互換性を保つことができる。従って、図 4

(a) に示すように、トランスポート層よりも上位の層

を暗号化層とし、さらにその上位層を、前述の転送諸元情報や原始暗号化情報を交換するセキュリティデータ交換プロトコル層とすれば、プロトコル互換性を保ちながら、転送される情報の秘匿性を保つことができる。

【0063】具体的には、図4(b)に示すように、LAP(データリンク層)、LMP(リンクマネージメント層)、及びTP(トランスポート層)のプロトコルデータユニットに続くサービス・データ・ユニットを暗号化すれば良い。従って、通信装置2及び通信装置3の双方において、赤外線通信リンクBを介して送受信する信号の暗号化及び復号を行うことにより、図3に示す処理で送受信される転送諸元情報や原始暗号化情報の秘匿性をより確実なものとすることができる。

【0064】図5は、図3に示す処理の実行後における通信装置2の動作を示すフローチャートである。この図5に示す処理において、通信装置2は、Bluetooth規格により規定されるMasterのデバイスとして動作する。また、図5に示す処理において送受信される無線信号は、Bluetooth規格に準じた2.4GHz帯の無線信号である。

【0065】まず、CPU21は、入力部23から入力される指示に従って動作を開始し、無線通信部24を制御してPage Scan動作を実行し、Bluetooth規格に準じた通信が可能な通信装置を検出する(ステップS41)。

【0066】そして、接続可能な通信装置を検出した場合は、CPU21によるPage Scan動作に応じて検出した装置から送信された情報を受信し(ステップS42)、受信した情報と、メモリ22内の原始暗号化情報格納領域101に格納されている原始暗号化情報との照合を行う(ステップS43)。

【0067】ここで、通信装置2が通信装置3を検出した場合、通信装置3は、メモリ22内の原始暗号化情報格納領域101に格納されている原始暗号化情報を既に保持しているため、Page Scan動作に応じて原始暗号化情報に従って暗号化された情報を送信する。また、通信装置2及び通信装置3とは無関係な通信装置が検出された場合は、この無関係な通信装置からは、Page Scan動作に応じて通常の無線信号が送信される。従って、ステップS43における照合により、ステップS41で検出した通信装置が通信装置3であるか否かを判別できる。

【0068】ステップS43における照合の結果、ステップS42で受信した無線信号が原始暗号化情報とは無関係であった場合は(ステップS44; No)、CPU21は、検出した通信装置との接続を拒否し(ステップS45)、本処理を終了する。

【0069】また、ステップS43での照合により、ステップS42で受信した無線信号が原始暗号化情報に適合した場合は(ステップS44; Yes)、CPU21は、検出した通信装置との間で、原始暗号化情報格納領域101内の原始暗号化情報により暗号化された無線信号の送受信を開始する(ステップS46)。なお、原始

暗号化情報格納領域101に格納された原始暗号化情報により暗号化された情報は、該原始暗号化情報をもとに復号できる。このため、CPU21は、無線通信部24により送信する情報を暗号化するとともに、無線通信部24により受信した情報を復号する。

【0070】そして、CPU21は、検出した通信装置との間のネゴシエーションが終了してからアプリケーションでの使用を許可する(ステップS47)。その後、CPU21は、通信装置2、もしくはインターフェース部28に接続された電子機器4上で実行されるアプリケーションプログラムの要求に応じて、暗号化された無線信号を送受信する処理を実行し(ステップS48)、入力部23からの指示入力によって本処理を終了する。

【0071】以上のように、本発明の第1の実施の形態によれば、Bluetooth規格に準じた無線通信を行う無線通信部24及びアンテナ25と、赤外線信号を用いた無線通信を行う赤外線通信部26及び赤外線受発光ユニット27とを備える通信装置2と、通信装置2と同一構成によってなる通信装置3との間において、予め赤外線通信によって原始暗号化情報を転送し、その後、転送した原始暗号化情報に基づいて暗号化された情報を、Bluetooth規格に準じた無線通信で送受信する。これにより、高い秘匿性を保ちながら、Bluetooth規格に準じた利便性の高い通信を行うことができる。

【0072】すなわち、Bluetooth規格に準じた無線通信を利用した場合、互いの通信装置を近接させるだけでピコネットを形成して通信を開始できる。また、通信中の各通信機器は、同時に他の通信装置との間においてピコネットを形成することができ、フレキシブルな通信を行うことができる。さらに、ピコネットを形成する通信装置は、互いに所定の距離以内に近接していれば良く、位置が拘束されることが少ない。その反面、Bluetooth規格に準じた無線通信では、特定の通信装置に対してのみ情報を送信することが難しく、誤って無関係な通信装置に受信されてしまう可能性が否定できない。しかしながら、上記第1の実施の形態における通信システム1によれば、予め通信装置2と通信装置3との間で、赤外線通信によって原始暗号化情報を転送することにより、無関係な通信装置に影響されることなく原始暗号化情報を共有し、この原始暗号化情報を用いて暗号化された情報を、Bluetooth規格に準じた無線通信で送受信する。従って、セキュリティ上の信頼性を確保しながら、利便性の高い無線通信を行うことができる。

【0073】なお、上記実施の形態においては、通信装置2と通信装置3とは、Bluetooth規格に準じた無線通信リンクAを介して無線通信を行うものとしたが、本発明はこれに限定されるものではなく、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に対しても適用可能であり、上記の通信システム1と同様の効果を奏するものである。

【0074】さらに、携帯型電話機やPDA、パーソナルコンピュータ、プリンタ、音楽プレーヤ等の各種電子機器に本発明を適用する場合は、図1に示したような通信装置2及び通信装置3に対して電子機器4、5が接続される構成に限らず、上記各種電子機器に、通信装置2、3の機能を内蔵させることも勿論可能である。

【0075】また、上記第1の実施の形態においては、通信装置2及び通信装置3はいずれも入力部23、33を具備しており、これら入力部23、33における指示入力によって図3に示す処理を開始するものとしたが、必ずしも入力部23、33を備える構成でなくても良い。以下、この場合について第2の実施の形態として説明する。

【0076】〔第2の実施の形態〕図6は、本発明の第2の実施の形態における通信システム10の構成を示すブロック図である。

【0077】同図に示すように、通信システム10は、通信装置2と、通信装置3aとによって構成される。通信システム10は、通信装置3aが有するメモリ61およびスイッチ62を除いては、上記第1の実施の形態における通信システム1と同様の構成によってなるものであり、共通部分については同符号を付して説明を省略する。

【0078】スイッチ62は、1個もしくは複数のスイッチを備えており、操作される毎に操作信号を生成してCPU31へ出力する。

【0079】図7は、メモリ61の内部構成を模式的に示す図である。同図に示すように、メモリ61内には、原始暗号化情報格納領域103及び転送諸元情報格納領域102が設けられており、転送諸元情報格納領域102には製品情報、固有機能情報、使用者情報、シリアルNo.等の転送諸元情報が格納されている。一方、原始暗号化情報格納領域103には、事前に原始暗号化情報は格納されていない。

【0080】上記第1の実施の形態で説明した通信システム1では、図3に示す処理において、通信装置2から通信装置3へ原始暗号化情報が転送され、メモリ22の原始暗号化情報格納領域101に格納されていた原始暗号化情報が、メモリ32の原始暗号化情報格納領域101に格納される。本第2の実施の形態における通信システム10では、通信装置2から通信装置3aへ原始暗号化情報が転送されると、転送された原始暗号化情報はメモリ61の原始暗号化情報格納領域103へ格納される。従って、通信装置3aは、上記通信装置3と同様に動作することができる。

【0081】また、上記第1の実施の形態で説明した通信システム1では、通信装置2が有する入力部23および通信装置3が有する入力部33における指示入力により、図3に示す処理が開始されるものとした。本第2の実施の形態における通信システム10では、通信装置2

が有する入力部23における指示入力、及び、通信装置3aが有するスイッチ62のスイッチ操作によって、図3に示す処理と同様の処理が実行される。

【0082】すなわち、通信装置3aは、入力手段としてスイッチ62のみを備える装置であるが、上記第1の実施の形態における通信装置3に代えて、通信装置2によるアクセスを受信する動作のみを行う装置として使用可能である。また、通信装置2に代えてアクセス要求側の装置として利用しないため、メモリ61の原始暗号化情報格納領域103には予め原始暗号化情報を格納する必要がない。

【0083】従って、本第2の実施の形態における通信システム10は、入力スイッチ62のみを有する通信装置3aを用いて、上記第1の実施の形態と同様の効果を奏するものである。これにより、Bluetooth規格に準じた無線通信において、Slaveのデバイスとしてのみ機能する装置には、入力手段としては単なるスイッチを備えるだけで、通信システム1と同様の効果を得ることができる。

【0084】

【発明の効果】請求項1記載の発明の通信装置によれば、送信される情報は、第2の通信手段によって送信された暗号化鍵情報を受信した通信装置でのみ受信可能となる。これにより、第1の通信手段による無線通信について、セキュリティ上の信頼性を確保することができる。特に、第1の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第2の通信手段によって送信される暗号化鍵情報を受信した通信装置のみに限定できる。従って、通信相手の装置との位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【0085】請求項2記載の発明の通信装置によれば、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報を保持していない外部の通信装置に対しては、通信拒否手段により、第1の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置を厳格に限定し、情報の秘匿をより確実に保持することができる。

【0086】請求項3記載の発明の通信装置によれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース (Bluetooth) 規格の無線通信において、情報の秘匿性を確保することができる。特に、第2の通信手段に赤外線信号を用いた通信方式を利用するので、第2の通信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能であ

る。また、赤外線信号を用いた通信方式では、通信装置は互いに近接し、かつ所定の立体角以内で対向する必要があるため、情報の秘匿性をより一層高めることができる。

【0087】請求項4記載の発明の通信システム、及び、請求項8記載の発明の通信方法によれば、送信側装置により送信される情報は受信側装置でのみ受信することができる。これにより、送信側装置が有する第1の通信手段を用いた通信システム内の無線通信について、セキュリティ上の信頼性を確保することができる。特に、第1の通信手段による無線通信が、例えばブルートゥース規格のように、仕様や規格が公開され、或いは広く普及して互換性が保たれている無線通信方式に準じたものである場合は、無関係な通信装置により受信されてしまう可能性が否定できない。しかしながら、本発明を適用すれば、通信の相手を、第2の通信手段によって送信される暗号化鍵情報を保持する受信側装置のみに限定できる。従って、互いの装置の位置関係が比較的自由である等、無線通信の利便性を損なうことなく、情報の秘匿性を保持し、セキュリティ上の信頼性を確保することができる。

【0088】請求項5記載の発明の通信システムによれば、送信側装置は、鍵情報保持手段に保持された暗号化鍵情報と同一の暗号化鍵情報が、受信側装置が有する受信鍵情報保持手段に保持されていない場合に、通信拒否手段によって、第1の通信手段による無線信号の送受信を拒否するので、通信の相手となる通信装置をより厳格に限定し、情報の秘匿性をより確実に保持することができる。

【0089】請求項6記載の発明の通信システムによれば、広く仕様が公開され、利便性に富む一方、確実な情報秘匿が困難なブルートゥース (Bluetooth) 規格の無線通信において、情報の秘匿性を確保することができる。特に、第2の通信手段と鍵情報受信手段とは赤外線信号を用いた通信方式を利用するので、第2の通信手段および鍵情報受信手段の小型化、軽量化、低コスト化および省電力化が可能であり、容易に実現可能である。また、赤外線信号を用いた通信方式では、送信側装置と受信側装置とは互いに近接し、かつ所定の立体角以内で対向する必要があるため、情報の秘匿性をより一層高めることができる。

【0090】請求項7記載の発明の通信システムによれば、送信側装置が有する鍵情報送信制御手段は、暗号化鍵情報を暗号化して第2の通信手段によって送信させるので、暗号化鍵情報を送信する際の情報の漏洩をより確実に防止できる。これにより、セキュリティ上の信頼性をより一層高めることができる。

【図面の簡単な説明】

【図1】本発明を適用した第1の実施の形態における通信システム1の構成を示すブロック図である。

【図2】図1のメモリ22、32の内部構成を模式的に示す図である。

【図3】図1の通信システム1の動作を示すフローチャートであり、(a)は通信装置2の動作を示し、(b)は通信装置3の動作を示す。

【図4】図3に示す処理に暗号化を施した場合のプロトコル構成を示す説明図であり、(a)は暗号化を施す際の赤外線通信におけるプロトコル構成を示す階層モデルを示し、(b)は、赤外線通信におけるデータユニットの構成を模式的に示す。

【図5】図1の通信装置2によりBluetooth規格に準じた無線通信を行う際の動作を示すフローチャートである。

【図6】本発明を適用した第2の実施の形態における通信システム10の構成を示すブロック図である。

【図7】図6に示すメモリ61の内部構成を模式的に示す図である。

【符号の説明】

1、10 通信システム

2、3 通信装置

21、31 CPU

22、32 メモリ

23、33 入力部

24、34 無線通信部

25、35 アンテナ

26、36 赤外線通信部

27、37 赤外線受発光ユニット

28、38 インターフェース部

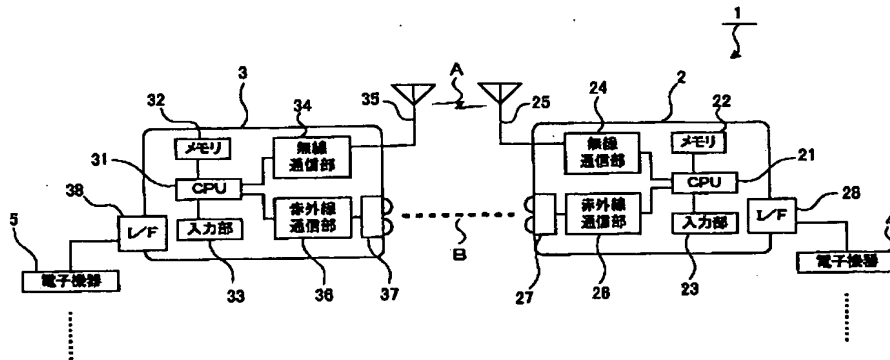
61 メモリ

62 スイッチ

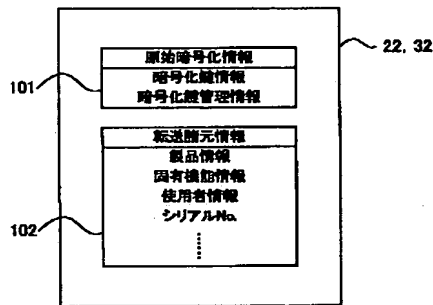
101、103 原始暗号化情報格納領域

102 転送諸元情報格納領域

【図 1】

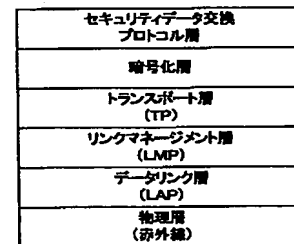


【図 2】

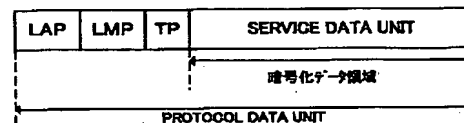


【図 4】

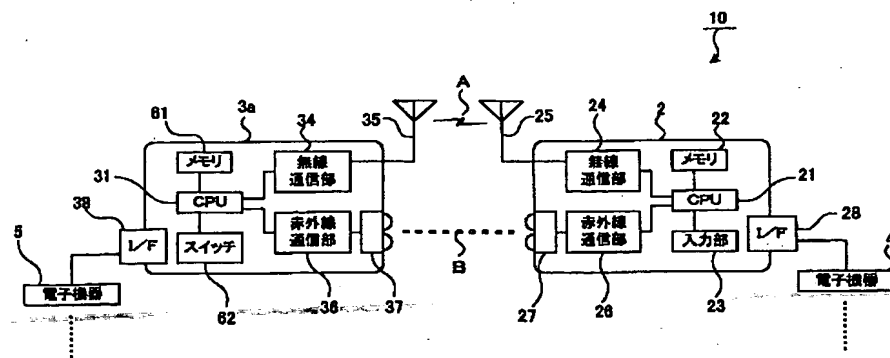
(a)



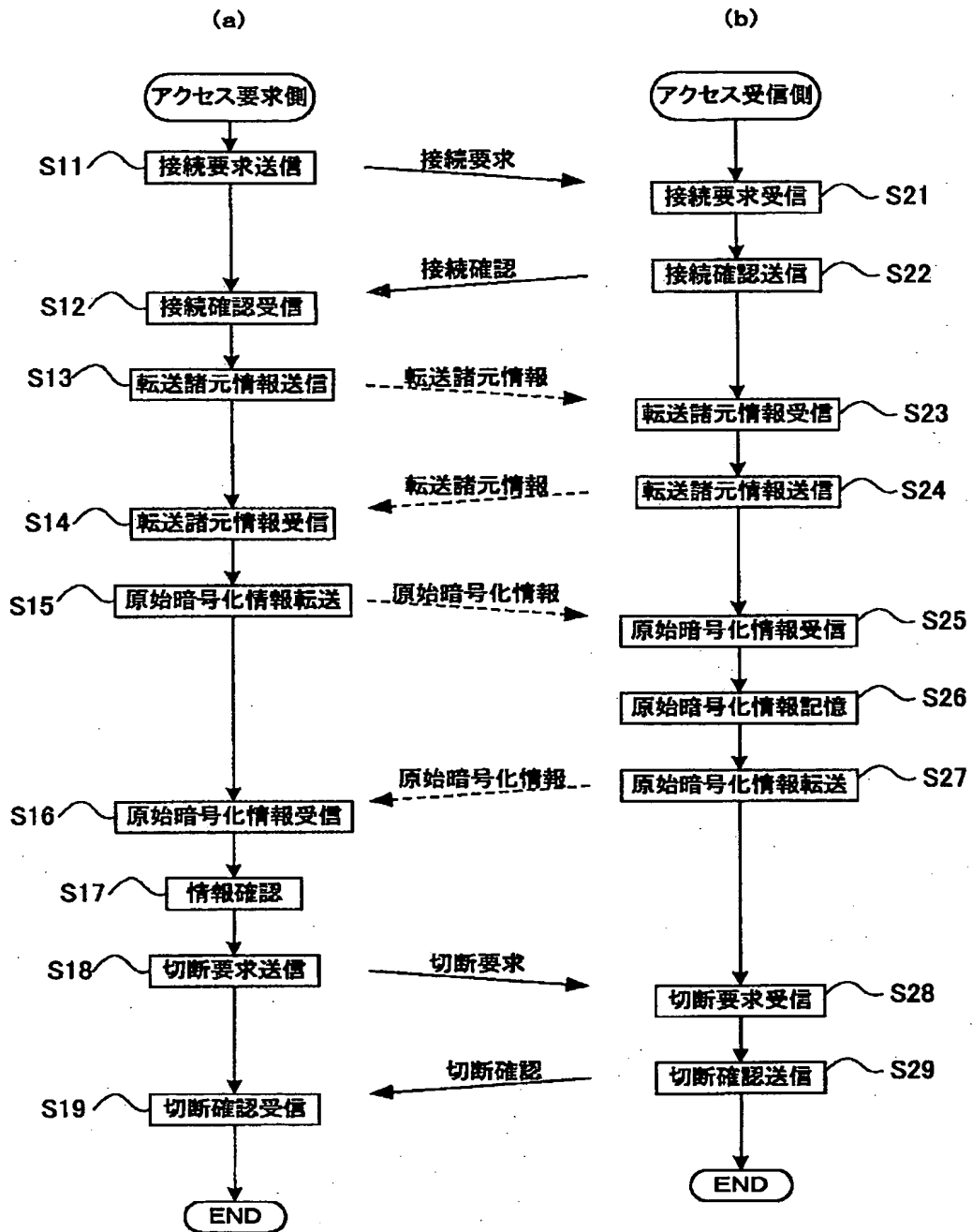
(b)



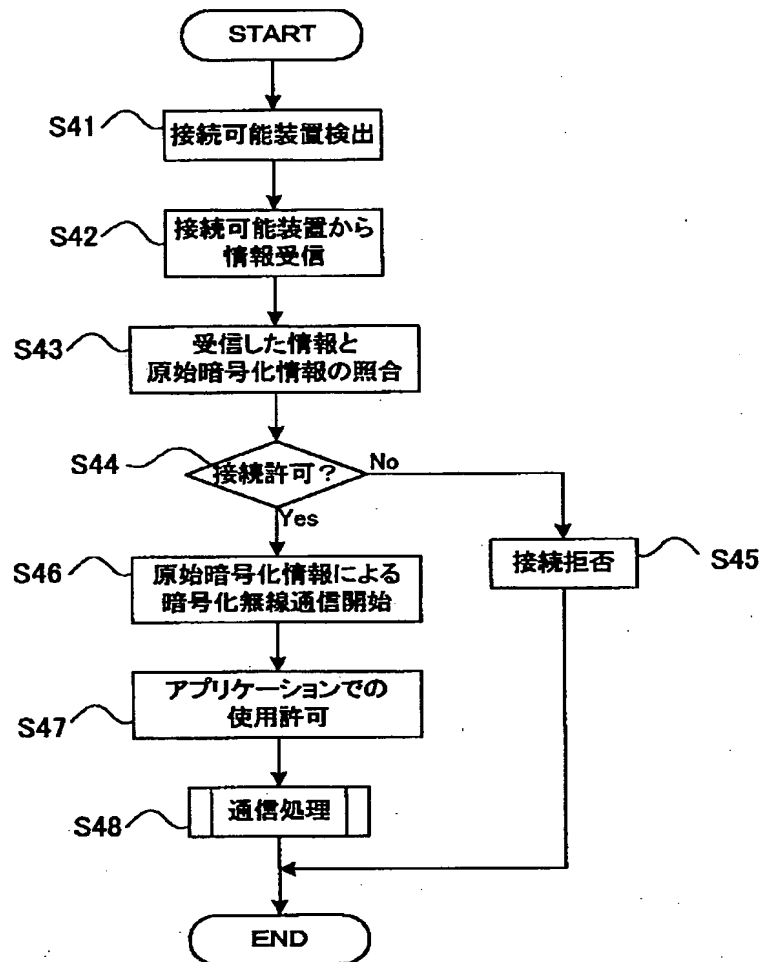
【図 6】



【図 3】



【図 5】



【図 7】

